UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/390,362	09/07/1999	SCOTT ALEXANDER VANSTONE	06944.0017	6724

22852 7590 08/28/2003

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 08/28/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/390,362	VANSTONE ET AL.	
	Examiner	Art Unit	
	Odaiche T Akpati	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: Page 1, line 20 has the phrase "problem with" that does not flow with the meaning of the sentence. The examiner assumes the phrase here is "goal of." Please refer to this problem and make the necessary corrections.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4, 5, 7, 10 recites the limitation "said one bit string" in lines 17, 19, 26, 36 respectively. There is insufficient antecedent basis for this limitation in the claim. Claims 5, 8, 9 and 10 inherit the rejection by virtue of dependency. Please make the necessary corrections. For the purpose of applying art, the examiner will interpret this phrase to mean "one of said bit strings."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP0918274A2) in view of Coron et al (XP-002193618).

With respect to Claim 1, the limitation "utilising one of said bit strings to compute a first signature component, forming from said first signature component and another of said bit strings an intermediate signature component, utilizing said intermediate component to provide a second signature component and combining first and second components with said other of said bits strings to provide a signature" is met by McCollum, column 3, lines 11-20. Please note that the word "fingerprint" in McCollom refers to "signature" as stated on column 1, lines 21-23. McCollom describes manipulation of data components to create a digital signature. McCollom however does not describe the message being split into two parts. Coron et al describes splitting a message into two parts on page 9, second paragraph.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Coron within the system of McCollom so as to be able to ensure integrity of the message when it is received.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP0918274A2) in view of Coron et al (XP-002193618) in further view of Menezes et al (Handbook of Applied Cryptography) in further view of Nyberg (0639907A1).

The combination of McCollom and Coron et al is already discussed in Claim 1 rejection. The combination of McCollom and Coron et al does not describe any redundancy being introduced into the message. Menezes however discusses redundancy in a message being transmitted. Menezes describes comparing message redundancy within a message to a

checksum, which is some form of predetermined level. Furthermore, Nyberg teaches on page 2, column2, lines 48-49 that validation of a message x can be based on some redundancy contained in x.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Menezes's teaching of redundancy into the combination of McCollom and Coron's teaching because of Nyberg's motivation that suggests that redundancy bits help with message validation.

Claims 3, 4, 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP0918274A2) in view of Coron et al (XP-002193618) in further view of Menezes et al (Handbook of Applied Cryptography) in further view of Nyberg (0639907A1) in further view of ISO/IEC FCD 9796-1.

With regards to Claim 3, the combination of McCollom, Coron and Menezes have already been discussed in Claim 2 rejection. The combination of McCollom, Coron and Menezes however does not teach about redundancy being introduced to exceed a predetermined level. The limitation "wherein said redundancy is adjusted to exceed said predetermined level" is taught by ISO/IEC FCD 9697-1 on page1, third paragraph, lines 12-14. The reference talks about the message being extended, which represents the excess bits that exceed the predetermined level. Redundancy being introduced into the message is also further discussed in the reference.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to add the teachings of ISO/IEC FCD 9697-1 to the combination of McCollom, Coron,

Menezes because the excess bits help in the verification process, where the redundancy needs to be revealed (ISO/IEC FCD 9796-1, page 1, third paragraph, lines 16-18), so that the message can be eventually retrieved.

With regards to Claim 4, the combination of McCollum, Coron, Nyberg and ISO/IEC FCD 9796-1 do not discuss data being added to the message for the purpose of adjusting the redundancy. However, Menezes inherently discloses this on page 363, first paragraph. It would have been obvious to one of ordinary skill in the art at the time of the invention to implement redundancy in the message teaching of Menezes within the combination of McCollom, Coron, Nyberg and ISO/IEC FCD 9796-1 because incorporation of redundancy bits into a message assists with message validation (Nyberg, page 2, column2, lines 48-49).

With regards to Claim 5, the combination of McCollum, Coron, Menezes and Nyberg do not discuss an indicator for showing that data has been added to the message. However this is inherent in the reference ISO/IEC FCD 9697-1 on page1, third paragraph, lines 16-18. Since redundancy in the message needs to be revealed by the verification process, there is inherently an indicator that would shows this.

It would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of ISO/IEC FCD 9697-1 to the combination of McCollum, Coron, Menezes and Nyberg because the detection of the redundancy bits in the message is necessary for message validation as taught by Nyberg on page 2, column2, lines 48-49, and it further helps

in the telling apart the message from the redundancy bits so that the message can be eventually extracted.

Claims 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coron et al (XP-002193618) in view of McCollom (EP0918274A2).

With respect to Claim 6, creation of the digital signature from the message bits is discussed in Claim 1. The limitation "wherein said second component is generated by hashing said first component and said other bit string" is met by McCollom on column 3, lines 11-20. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of McCollom within the system of Coron because message hashing is a necessary step in the creation of a digital signature.

Claims 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP0918274A2) in view of Coron et al (XP-002193618) in further view of Kitaori et al (5915024).

With respect to Claim 7, the limitation "including at least one component having only one of said bit strings encrypted therein, and the other of said bit strings, said method comprising the steps of combining said one component with the other bit string, recovering said one bit string from said combination" is met by McCollom, column 3, lines 11-20.

The limitation "examining said recovered one bit string for a predetermined characteristic" is inherent in McCollom, column 3, lines 11-20.

McCollom however does not describe the message being subdivided into a pair of bit strings, nor does he talk about using information of the signer towards the digital signature process. Coron talks about a message being subdivided into two parts.

The limitation "a method of verifying a message subdivided into a pair of bit strings from a signature" is met by Coron et al, page 9, second paragraph.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Coron to that of McCollom because subdividing the message into two parts enables the creation of a more secure digital signature.

The combination of McCollom and Coron however do not describe the usage of the information of the signer towards the digital signature process. Kitaori discusses this as described below.

The limitation "using publicly available information of the purported signer" is met by Kitaori et al on column 9, lines 28-30.

It would be obvious to one of ordinary skill in the art to add Kitaori's teaching to the combination of McCollom and Coron's teaching so as not to lose the validity of the message, as discussed in Kitaori et al on column 8, lines 61-65.

Claims 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP0918274A2) in view of Coron et al (XP-002193618) in further view of Nyberg (0639907A1) in further view of Kitaori et al (5915024).

With regards to Claim 8, the combination of McCollom, Coron and Kitaori do not expressly disclose hashing of the signal component and bit string. Even though McCollom does

not discuss hashing, he talks about encryption of the combined signal on column 3, lines 17-18. Nyberg, furthermore, expressly discusses hashing in digital signatures on column 2, lines 49-56. Hence, hashing can be intuitively substituted for the encryption step in McCollom since it is a form of an encryption process, and furthermore, a necessary part of obtaining a digital signature.

It would be obvious to one of ordinary skill in the art at the time the invention was made to incorporate hashing teaching of Nyberg into the combination of McCollom, Coron and Kitaori's teaching because hashing is a necessary, common step in the process of obtaining a digital signature.

Claims 9, 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom (EP0918274A2) in view of Coron et al (XP-002193618) in further view of Kitaori et al (5915024) in further view of Nyberg(0639907A1).

With regards to Claim 9, the combination of McCollom, Coron, Kitaori and Nyberg have been discussed in Claim 8. However, the combination of McCollom, Coron and Kitaori does not describe redundancy as part of the digital signature process. Nyberg however discusses this as shown below.

The limitation "wherein said predetermined characteristic is the redundancy of said recovered one bit string" is met by Nyberg, column 2, lines 48-49. It would have been obvious to one of ordinary skill in the art to add the teachings of Nyberg to the combination of McCollom, Coron and Kitaori because redundancy is very useful for message validation.

With regards to Claim 10, the combination of McCollom, Coron, Nyberg and Kitaori are already discussed in Claim 9. However, the combination of Coron, Kitaori and Nyberg do not explicitly describe any manipulations on the message bits to derive the signature. This is however disclosed in McCollom. The limitation "said signature includes a second component derived from a combination of said one component and said other bit string and said one bit string is recovered utilizing said second component" is met by McCollom, column 3, lines 11-20. It would be obvious to one of ordinary skill in the art at the time the invention was made to add the teaching of McCollom to the combination of Coron, Kitaori and Nyberg because the manipulations of the message parts help in obtaining a secure digital signature.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Odaiche Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7240 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

***

August 22, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100